Blockchain consensus: From proof-of work to proof-of-stake

Jonathan Healy
jonathan.d.healy@gmail.com
January 2020

1. Introduction

With the introduction of Bitcoin in 2008 via the Bitcoin white paper [1], written by an author cloaked in anonymity – Satoshi Nakamoto - the notion of the blockchain was released on the world. The consensus model for this new concept was, and still is, generally called proof-of-work. Nodes in the network seeking to acquire rewards, associated with adding a block of transactions to the inter-connected chain of blocks that stretch right back to the very genesis block itself, compete to compute cryptographic puzzles. After a valid block of transactions is assembled and a hash containing enough leading zeroes is found for that block, the block is examined by other nodes in the network. If everything checks out, the block is added to the blockchain and other blocks will henceforth be added to it.

Consensus is important here, of course, because the system relies on it to provide security and ensure that the double-spending problem is solved. Solving this problem guarantees that the same unit of currency will not be spent twice. Prior to the introduction of Bitcoin this was something that was unsolved in a decentralized network. Previous solutions all relied on the existence of a central authority providing accountability. Over the years confidence in Bitcoin has grown and today the network has a market cap of over $157 billion dollars, measured in US currency. There are two main criticisms of Bitcoin, however.

One criticism of Bitcoin is that the network is slow and the other concerns the vast amounts of energy via electricity that is presently being used to secure the Bitcoin blockchain. Both of these things can potentially be addressed by improving Bitcoin's consensus model.

The most popular idea with respect to replacing proof-of-work is easily, proof-of-stake. In this system, nodes are generally chosen to validate a block of transactions and receive the corresponding reward with the odds of doing so being based on the number of tokens that are held in a node's account [2, 4]. Pure proof-of-stake is a recent modification to proof-of stake that seeks to eliminate some of the major criticisms directed at previous proof-of-work iterations [2]. The last blockchain consensus model that will be looked at is federated byzantine agreement [3]. Consensus in this model is carried out via trusted participants and does not rely on the number of tokens that a validator has – proof-of-stake – or the amount of hash power that a validator can produce – proof-of-work.

2. Proof-of-Work (PoW)

Proof-of-work is a concept that has become famous via Bitcoin but it was not a new idea as of the publication of [1]. Hashcash [5] was originally proposed in 1997 as a means to, "throttle systematic abuse of un-metered internet resources such as email and anonymous remailers." Hashcash was described as a trapdoor-free cost function meaning that is was a cost function where a server would have no advantage in minting tokens. The idea is that by requiring proof-of-work, illegitimate entities would be unable to expend the effort needed to send out large amounts of spam. Interestingly one of the applications envisioned in [5] was as a minting mechanism for b-money which was proposed by Wei Dei [6] and is generally thought of as the precursor to Bitcoin.

3. Proof-of-Stake (PoS)

Unlike proof-of-work, proof-of-stake does not rely on solving difficult cryptographic puzzles in order for the network to reach consensus. There are many proposed ways to implement proof-of-stake but the general idea is that validators are chosen to lead any round with the odds stacked in their favor via the number of tokens that they hold. One popular offshoot is delegated proof-of-stake (DPoS). In DPoS there are only a certain number of validators in the network and token holders can vote for those validators by delegating their tokens to them.

One PoS proposal receiving a lot of attention is [4] as it being developed by the team behind Ethereum. Their PoS scheme – Casper - has been partially derived from Byzantine fault tolerance (BFT) literature. BFT algorithms can generally be proven to reach consensus if more than 2/3 of all validators are honest, regardless of network latency. Interestingly, [4] is designed as an overlay for PoW systems like Ethereum in order to offer PoS based security improvements. Casper is initially responsible for finalizing blocks while the underlying PoS consensus mechanism is responsible for proposing blocks. If attackers fully control the proposal mechanism, Casper can prevent the network from finalizing two conflicting checkpoints. Attackers however could prevent Casper from finalizing future checkpoints.

Implementing Casper on Ethereum is intended to eventually lead to fully replacing the underlying PoW proposal mechanism. Casper introduces the idea of slashing to combat undesirable behaviour in the network. PoS validators would have their stake locked away and their balances could be either diminished or even fully eliminated by the protocol. Punishing nodes is supposed to allow for things like accountability which is something that BFT algorithms generally don't support. The authors in [4] suggest that other PoS implementations are plagued by the 'nothing at stake' problem where attackers can keep attacking the system from within without fear.

By punishing stakeholders, it is claimed that Casper provides stronger security incentives than PoW even. Volunteering to lock away one's funds however might be a risky proposition. Having an attacker trick your computer into following the wrong chain could have catastrophic consequences. Validators would have to have complete trust in the system and this could affect the overall security of the network as many honest participants may choose to not participate. A discovered security flaw may lead to a large number of dishonest attackers joining the system.

4. Pure Proof-of-Stake (PPoS)

Algorand is a blockchain protocol headed by former Turing award winner Silvio Micali. Algorand uses an alternate version of proof-of-stake called pure proof-of-stake (PPoS). Although Algorand has evolved since the paper, 'Algorand: Scaling Byzantine Agreements for Cryptocurrencies' was published in 2017 the basics surrounding the protocol can be found in it [2].

Algorand implements a new Byzantine Agreement protocol to establish consensus. Verifiable Random Functions are used which allow network nodes to privately check if they have been selected to participate in assembling a new block. This same mechanism allows for nodes to include a proof of their selection in their network messages. Users therefore do not need to keep any private state except for their private keys which helps improve general security.

The protocol allows Algorand to replace participants immediately after they send a message. This helps PPoS to differentiate itself from most regular proof-of-stake schemes. In many implementations of PoS, prospective validators need to lock their funds into the system. Algorand allows Users to have free access to their funds while also enjoying the benefit of potentially receiving rewards for being chosen as a block validator. Having a larger pool of validators to choose from via the utilization of Verifiable Random Functions improves security because attacks carried out on a chosen group of validators is not as concerning anymore.

Results published [2] state that Algorand achieves a throughput over 125x greater than what can be achieved by Bitcoin with much faster block confirmation times to boot. Furthermore, the

authors state that the network receives almost no penalty for scaling. The Algorand MainNet was launched in June 5 of 2019.

5. Federated Byzantine Agreement

Federated Byzantine Agreement (FBA) is a consensus model introduced to the world by Stanford professor David Mazieres in the paper, 'The stellar consensus protocol: A federated model for internet level consensus' published in 2015 [3]. Federated Byzantine Agreement differs from proof-of-stake because consensus is not carried out by nodes chosen with weight given to the number of tokens that they hold in the native currency.

In FBA, each participant or validator selects a subset of other nodes that it trusts and this group is sometimes called a, 'quorum slice'. After considering a transaction, a participant waits for the vast majority of the nodes that it trusts to signal that they agree with the transaction. The nodes that the participants trust also have other nodes that they trust and they wait for those other nodes to decide before making their own decision on any transaction. In this way, the whole network soon agrees on a transaction and it becomes infeasible for an attacker to roll back a transaction. Stellar is a public blockchain network built on the FBA consensus model. To become a validator in the network and bootstrap into the system a participant just needs another validator to add them to their quorum slice.

7. Conclusion

Contrary to common belief, consensus is not an avenue that is closed to further research. The emergence of Bitcoin opened the world to the possibility for new types of distributed systems. This realization extended even beyond those interested in a public, decentralized model like that which was offered by Bitcoin. Blockchains have been proposed for many types of applications. Industries have adopted these ideas to create permissioned networks where participants are semi-trusted. Proof-of-work as adopted by Bitcoin has proven to be slow – to prevent forking – and energy inefficient. Proof-of-stake is still a new concept that has not been tested yet extensively in the public arena. Proof-of-stake as proposed by Ethereum has been criticized for locking away funds with the ever-present threat of losing those funds because of bad behaviour. This is potentially a problem because there would be no one to complain to if there was an error in code. Algorand with their Pure Proof-of stake approach has announced that they have solved the problems surrounding other Proof-of-stake schemes by allowing validators to leave the system whenever they want and eliminating the need to punish validators and slash their balances. Algorand however is still relatively new and needs more time to be tested. One major criticism of both proof-of-work and proof-of stake surrounds the issue of centralization. As bitcoin has developed mining power has become extremely centralized and the vast majority of consensus in the network is carried out by just a few corporations. Proof-of-stake, it can be argued, is also far from decentralized as nodes with more stake in the system have higher odds of being chosen to validate blocks. In either model, if a nemesis controls the majority of the network, there could be disastrous results as a consequence. Some may point to game theory, thinking that a stakeholder attacking their own network would not happen because any attack on the network would likely cause the market price to crash long before they could sell enough tokens to compensate for their losses. This could be true, generally, but remember, we live in a world where governments, banking institutions, and even banking conglomerates like the Federal Reserve have at various times felt threatened by crypto-currency. The reason that Bitcoin was so exciting was that for a while it seemed like it was a truly decentralized system. Creating a truly decentralized system would invariably rely on the emergence of a brand-new consensus model. Federated Byzantine Agreement as a consensus model is interesting and solves some of the centralization concerns associated with PoW and PoS. However, because corporations in the network have become the most common 'trusted' entities it can't be considered to be the perfect system. Historically, governments and corporations have colluded, even in the United States, and even when such collusion is highly illegal. Proof-of-elapsed (PoET) time is an interesting invention that at first glance seems to level the playing filed by allowing anyone with a properly equipped Intel processor the opportunity to participate but obviously large companies would eventually start buying 1000s of such processors and controlling the network again. It does improve

on PoW as presently electricity costs and the need for expensive ASIC hardware prevent the average User from participating and adding to network security.

Solving the consensus problem for a permission-less public blockchain like Bitcoin or Ethereum that demands a decentralized solution is a computer science problem with sociological, political and economic implications. Other consensus models for other types of networks where decentralization is not the chief concern will also continue to be researched and improved upon. Choosing the right consensus model not only effects security but also transaction speed and throughput.

References

1. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.
2. Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." Proceedings of the 26th Symposium on Operating Systems Principles. 2017.
3. Mazieres, David. "The stellar consensus protocol: A federated model for internet-level consensus." Stellar Development Foundation 32 (2015).
4. Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." *arXiv preprint arXiv:1710.09437* (2017).
5. Back, Adam. “Hashcash: A denial of service counter-measure (2002).
6. W. Dai, “b-money,” http://www.weidai.com/bmoney.txt, 1998.
7. Corso, Amie. "Performance Analysis of Proof-of-Elapsed-Time (PoET) Consensus in the Sawtooth Blockchain Framework." (2019).